Dr Debi Ashenden
Centre for Cyber Security & Information Systems
Cranfield University
Defence Academy of the UK
Shrivenham, Swindon, SN6 8LA

Your Employees: The Front Line in Cyber Security

What happens if you lose trust in the systems on which you rely? If the displays and dashboards tell you everything is operating normally but, with your own eyes, you can see that this is not the case? This is what apparently happened with the Stuxnet virus attack on the Iranian nuclear programme in 2010.

While the technological effects of the Stuxnet virus on the Iranian nuclear programme have been widely reported, what hasn't been examined is how the attack seemed to have a subsidiary aim of making the Iranians distrust their own instruments and to make them doubt what they were seeing. This was arguably the first major attack on an industrial control system from a hostile threat agent but, as we can see, the impact went beyond physical destruction – it led to doubt and mistrust in the system to the extent that the Iranians ended up putting people in the plant to physically watch and report back on what was happening.

While Stuxnet seems to have been a nation state attack on a system, we have seen insider attacks on SCADA systems in the past. The first major incident of this nature was an attack on radio-controlled sewage equipment in Queensland in 2000. In this case the motivation for the attack was revenge. A disaffected ex-employee decided to get even and by issuing radio commands to the equipment that he was familiar with (and may well have helped to install) he caused 800,000 litres of raw sewage to flood parks, rivers and even the grounds of a Hyatt Regency hotel.

The number of cyber attacks on SCADA and manufacturing plants is fortunately still low but the potential scale of impact has focused attention on how we can protect such systems. The emphasis has been on addressing technical vulnerabilities. Increasingly there is technology in such plants that is connected to the Internet (usually for maintenance purposes) and this is likely to increase with the proliferation of Internet of Things (IoT) devices (for example, building management systems). Coupled with this is the recognition that many back end or Operational Technology (OT) systems were never designed with security in mind. These systems are often difficult to patch or update and it may not be practical to take them offline to patch vulnerabilities. The OT may also be connected to the Enterprise System (ES) that runs the business side of the organisation. This gives an attacker a pathway from one side of the business to the other, safety-critical, side of the operation.

Last year saw at least two further attacks that are worth mentioning, although there is relatively little detailed information available. In Norway, a number of oil and energy companies were targeted. Statoil were under attack for three days when their Intrusion Detection Systems flagged up that rogue code was being downloaded onto their system. A second attack last December was carried

out on a German steel plant. It seems that hackers gained access to control systems in the plant so that parts of the plant failed and a furnace couldn't be switched off.

The Insider Threat

Let's cast our eyes back over the attacks that have occurred. The attack on the German steel plant seems to have been caused by a spear phishing attack. These are targeted attacks, usually delivered via an email that has been personalised in some way. The employee receives an email that is specific to them but when they open it they unwittingly launch some rogue code onto the network. Another way of carrying out this type of attack is via a USB stick dropped, apparently dropped by accident, in a car park. Someone finds the USB stick and in an effort to be helpful (or just curious) plugs it into a computer to see if there's some indication of ownership. In the process the rogue code jumps from the USB stick onto the network.

It seems likely that Stuxnet got onto the Iranian nuclear system in a similar way. In this case though rather than a USB stick the code jumped from a laptop used by a maintenance engineer. The virus had got onto the laptop and the laptop was then connected to the system, allowing the virus the opportunity to jump off the laptop and onto the system it was programmed to attack.

Generally then it seems that one of the easiest ways to get malware onto process control systems is to exploit the links that are made between these systems and the Internet – or where the Enterprise System is connected to the Operational Technology.

Practical Steps to Manage the Risk

In an ideal world there should be an air gap between the Enterprise System and Operational Technology, between critical systems and the Internet. Sometimes, however, this simply isn't practical or, even if there is a policy against such connections employees will inadvertently or maliciously bridge these air gaps. So, what can you do to minimise the risk of this happening?

If you have a strong safety culture and you've tried using the model that support it as a way to improve your security culture you may have come across some difficulties. One of the key differences between safety and cyber security is that the riskiness of cyber security behaviours depends a great deal on the context in which they are carried out.

For example, the first step in changing organisational behaviour is identifying the specific behaviour that you want to change. From a safety perspective this could be holding onto a handrail while you go down some stairs. This is a very specific behavioural requirement. An equivalent behaviour from a security perspective might be locking your computer screen when you are away from your desk, or not using a USB stick (and you can physically prevent the latter by blocking USB

ports). Unfortunately though, many security behaviours are far harder to define in such a specific way – which in turn means it is more difficult for employees to understand exactly what they should do.

Hopefully it is easy to see from what we've discussed so far that not opening phishing emails would be a good security behaviour to establish. It is, however, difficult to define a specific behaviour that will stop employees falling victim to phishing attacks. If it was obvious that an email was a phishing email an employee wouldn't open it in the first place, but the skill in launching a phishing attack is that the email will look innocuous. If you ask employees not to open emails if they don't recognise the sender address or if they have other suspicions about it, then you could bring your organisation to a halt with important emails that aren't opened. Employees will, quite rightly, want to know what criteria to use for judging the validity of an email, and how long will you expect them to spend on making a decision about whether to open it or not? As you can see this is not a straightforward behavioural proposition.

So how can we minimise the risk of employees opening a phishing email? One way that is quite popular at the moment is to use a software tool that launches phishing emails against your employees but under your control. This will test whether your employees are likely to fall prey to a phishing attack. This sounds like a good idea and is fairly easy to do, however, there can be significant drawbacks.

Firstly, if you phish employees and they fall prey to it (and perhaps even get a telling off as a result, or, at best, some remedial security training) they may be less interested in trying to help you improve security. Nobody likes to get things wrong and many people feel that they've been tricked in this situation. The other danger is that they will start to exhibit signs of 'learned helplessness'. This is a psychological condition where an individual feels that there is little point in trying to do the right thing because they just can't win. At best you may get apathy around security behaviours and at worst, outright rejection.

<u>Turning Employees Into A Security Asset</u>

As with all technological approaches to solving an organisational problem the difference between success and failure depends on what sits around the technology. If you are going to use a software tool that enables you to phish your employees then it should only be one part of your behavioural change programme and you need to consider the following:

(i) Get your employees onside first by explaining what you're doing and why. The most productive way to do this is to have an open dialogue with them about security issues – and by dialogue I mean just that, speaking but also listening and exchanging ideas. What is the perception of cyber security risk in your organisation – do some employees think that cyber security requirements are over-hyped? Are parts of your organisation vulnerable to the 'culture of the expert' – you probably have very talented engineers and scientists in your organisations but they may also think they know better than you do about security. You might believe that you know how your employees think but your

first step should be getting out there and asking them, because it is very likely that you will get some opinions that you would never have second guessed.

(ii) Plan very carefully what you are going to do when employees open the phishing emails that you send. There will probably be a temptation to punish them in some way and insist that they do some further awareness training. This should be the last resort. The majority of employees want to do the right thing and most believe that they can make a contribution to organisational security. You need to foster this. The messages that you put out at this stage need to demonstrate that you understand that. Rather than a security expert talking down to an employee (in a kind of parent/child relationship) you should be having a peer-to-peer conversation. You are aiming to build the employee's feelings of 'self-efficacy' - this is the belief that they have in their own abilities to successfully manage a situation.

(iii) Recognise good behaviour when you see it. Security practitioners are often very quick to discipline employees for poor security behaviours but are less likely to praise or offer rewards for good security behaviours. This could be something as simple as an email of recognition to the employee's line manager.

(iv) Ideally what you are aiming for is a well thought through campaign where the launch of the phishing tool only forms one part. The other parts will be made up the dialogue that you have with employees where you explain the problems with phishing, the impact it could have and what you propose to do but, in turn, you also listen to their thoughts and ideas for how to address the situation. You will have a plan for those employees who fall prey to your phishing attacks that will increase their self-efficacy rather than leading them into learned helplessness. Finally, when employees exhibit good security behaviours (for example, when they report phishing emails to you for investigation) you should have a system for rewarding and recognising their behaviour.

The Future

While there have been relatively few attacks to date on industrial controls systems we have no reason to assume that this will continue. When we cast forward over the next five years analysts' predictions suggest that the attack surface will increase significantly. Gartner believes that by 2018, 6 billion 'things' will be connected to the Internet and a number of these will be able to request support for themselves (we already see examples of this with security systems that alert a security company that an alarm has been tripped). This means that the number of security events and attacks will rise and there will be a corresponding pressure on resources, both technological and human to manage this risk.

In short, the attack surface is getting bigger and technology cannot handle all the attacks that are being registered. We can use technology to prevent some of these through surveillance and monitoring but there is more we can do. Firstly, we can try to limit the instances of employees inadvertently causing a security breach and secondly, we can harness the goodwill and aptitude of our employees to take a more active role in preventing malicious attacks.

This work was part funded by the Centre for Research and Evidence on Security Threats (ESRC award, ES/N009614/1)